

APEC PRIVACY PRINCIPLES

**CONSULTATION DRAFT
31 MARCH 2004**

CONTENTS

Part I. Preamble

Part II. Scope

Part III. APEC Privacy Principles

Part IV. Implementation [to be discussed]

APEC PRIVACY FRAMEWORK

Part I. Preamble

APEC economies recognize the importance of protecting information privacy and maintaining information flows among economies in the Asia Pacific region and among their trading partners. As APEC Ministers acknowledged in endorsing the 1998 Blueprint for Action on Electronic Commerce, the potential of electronic commerce cannot be realized without government and business cooperation “to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy...”. The lack of consumer trust and confidence in the privacy and security of online transactions and information networks is one element that may prevent member economies from gaining all of the benefits of electronic commerce. APEC economies realize that a key part of efforts to improve consumer confidence and ensure the growth of electronic commerce must be cooperation to balance and promote both effective information privacy protection and the free flow of information in the Asia Pacific region.

Information and communications technologies, including mobile technologies, that link to the Internet and other information networks have made it possible to collect, store and access information from anywhere in the world. These technologies offer great potential for social and economic benefits for business, individuals and governments, including increased consumer choice, market expansion, productivity, education and product innovation. However, while these technologies make it easier and cheaper to collect, link and use large quantities of information, they also often make these activities undetectable to individuals. Consequently, it can be more difficult for individuals to retain a measure of control over their personal information. As a result, individuals have become concerned about the harmful consequences that may arise from the misuse of their information. Therefore, there is a need to promote and enforce ethical and trustworthy information practices in on- and off-line contexts to bolster the confidence of individuals and businesses.

As both business operations and consumer expectations continue to shift due to changes in technology and the nature of information flows, businesses and other organizations require simultaneous input and access to data 24-hours a day in order to meet customer and societal needs, and to provide efficient and cost-effective services. Regulatory systems that unnecessarily restrict this flow or place burdens on it have adverse implications for global business and economies. Therefore, in promoting and enforcing ethical information practices, there is also a need to develop systems for protecting information privacy that account for these new realities in the global environment.

APEC economies endorse the principles-based APEC Privacy Framework as an important tool in encouraging the development of appropriate information privacy protections and ensuring the free flow of information in the Asia Pacific region.

This Framework, which aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines)¹, and reaffirms the value of privacy to individuals and to the information society.

The Framework specifically addresses these foundation concepts, as well as issues of particular relevance to APEC member economies. Its distinctive approach is to focus attention on practical and consistent information privacy protection within this context. In so doing, it balances information privacy with business needs and commercial interests, and at the same time, accords due recognition to cultural and other diversities that exist within member economies.

The Framework is intended to provide clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted. It does so by highlighting the reasonable expectations of the modern consumer that businesses will recognize their privacy interests in a way that is consistent with the Principles outlined in this Framework.

Finally, this Framework on information privacy protection was developed in recognition of the importance of:

- Developing appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;
- Recognizing the free flow of information as being essential for both developed and developing market economies to sustain economic and social growth;
- Enabling global organizations that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;
- Enabling enforcement agencies to fulfill their mandate to protect information privacy; and,
- Advancing international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.

¹ The 1980 OECD Guidelines were drafted at a high level that makes them still relevant today. In many ways, the OECD Guidelines represent the international consensus on what constitutes honest and trustworthy treatment of personal information.

Part II. Scope

Definitions

personal information means any information about an identified or identifiable individual.

[personal information controller means a person or organization who controls the collection, holding, processing or use of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process or use personal information, but excludes a person or organization who collects, holds, processes or uses personal information based only on instructions received from another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in the course of personal activity of a domestic nature.]

publicly available information means personal information about an individual that the individual knowingly makes or permits to be made available to the public, or is legally obtained and accessed from:

- a) government records that are available to the public;
- b) journalistic reports; or
- c) information required by law to be made available to the public.

Application

In view of the differences in social, cultural, economic and legal backgrounds of each member economy, there should be flexibility in implementing these Principles.

Exceptions to these Principles contained in Part III of this Framework, including those relating to national sovereignty, national security, public safety and public policy should be:

- a) limited and proportional to meeting the objectives to which the exceptions relate; and,
- b) (i) made known to the public; or,
(ii) in accordance with law.

Part III. APEC Information Privacy Principles

1. Preventing Harm

Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

2. Notice

Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:

- a) the fact that personal information is being collected;
- b) the purposes for which personal information is collected;
- c) the types of persons or organizations to whom personal information might be disclosed;
- d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;
- e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.

All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.

It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information.

3. Collection Limitation

The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

4. Uses of Personal Information

Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:

- a) with the consent of the individual whose personal information is collected;

- b) when necessary to provide a service or product required by the individual; or,
- c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

5. Choice

Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.

6. Integrity of Personal Information

Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.

7. Security Safeguards

Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

8. Access and Correction

Individuals should be able to:

- a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;
- b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;
 - i. within a reasonable time;
 - ii. at a charge, if any, that is not excessive;
 - iii. in a reasonable manner;
 - iv. in a form that is generally understandable; and,
- c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

Such access and opportunity for correction should be provided except where:

- (i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;
- (ii) the information should not be disclosed due to legal or security reasons [or to protect confidential commercial information]; or
- (iii) the information privacy of persons other than the individual would be violated.

If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.

9. Accountability

A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.